REMARKS/ARGUMENTS

Claims 15-27 remain in this application.

Claims 15-27 have been added to obviate the rejections by the Examiner under 35 U.S.C. 112.

The Examiner has rejected Claims 1, 5, 7, 10 and 14 as being unpatentable over Richmond in view of Jerrim. Applicant respectfully traverses this rejection.

Referring to Richmond, there is taught controlling concurrent usage of network resources by multiple users at an entry point to a communications network based on identities of the users. Richmond teaches a plurality of users are connected to an entry point of a network by a shared transmission medium. For each of the one or more users, packet rules may be provisioned to the user's entry point to the network where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user for any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provision to the user's entry point in response to the user being authenticated. See paragraphs 109 and 110.

From the above description, and a complete review of Richmond, it is evident that there is no consideration of the possibility of an intruder. Richmond simply discusses whether a user has authorization or not. Richmond does not recognize the situation that intruders can exist who are unauthorized and still obtain access to and consequently compromise networks. Richmond makes the assumption that if the user does not have any authorization, nothing more will happen. Applicant's claimed invention specifically deals with the situation that there is going to be an intruder, and limits the intruder so the access the intruder has is extremely limited.

Claim 1 has the limitation that the second node cannot use any port between the first and third nodes except for the first and second TCP/IP ports, which prevents an intruder who compromises the second network from gaining access to the first network except for the first TCP/IP port. Richmond does not teach or suggest this limitation.

Furthermore, Richmond does not teach or suggest, and is silent in regard to the limitation that the second node only communicating with the first port of the first node through the communication portion via TCP/IP port extension using Gateway methodology which does not connect the first network with the second network.

Referring to Jerrim, there is disclosed network service zone blocking. Jerrin teaches monitoring for the presence of unauthorized applications and unauthorized activity is important. Fire walls merely limit access between networks in commercially available intrusion detection systems, a stream of bytes being transmitted is analyzed for certain strings of characters in the data commonly referred to as signatures. These signatures are particular strings that have been discovered in known exploits. Another approach to intrusion detection includes detection of unusual deviation from normal data traffic commonly referred to as anomalies. See paragraphs 7, 8, 9, 10 and 11. Failure to detect the operation of malicious unauthorized applications, such as a Trojan Horse can cause serious harm to a company. See paragraph 14. Unauthorized network usage can also be harmful. Employees may waste time and resources by installing and playing games over the network. An authorized website may utilize crucial bandwidth by providing materials such as pictures, streaming audio or movies. See paragraph 15.

Filtering tables in a local area network bridge device may allow a system administrator to block communications between particular hosts with other hosts physically connected to different local area network segments. Filtering tables inhibit forwarding of frames between particular

sets of medium access control protocol addresses between local area networks. See paragraph 16.

Jerrin teaches a monitoring system is needed that can detect the operation of unauthorized network services. The system needs to be able to differentiate between legitimate network usage and unauthorized activity. Additionally, the system needs to be able to control unauthorized network usage behind a systems firewall. See paragraph 17.

Jerrin teaches detecting unauthorized network issues based upon zone locking which can be implemented in conjunction with a port profiling system. See paragraph 18. Unauthorized network service is detected by a port profiling engine that monitors activity to differentiate between abnormal activity in normal communications. The port profiling engine does not rely on analyzing the data packets for signatures of known attacks. Instead, the monitoring system inspects inbound and outbound activity and identifies the services utilized by the house. Upon identification of the house, the system determines the zones of the host participating in the network communication. The system alarms on detection of communications between zones that are not authorized.

From the above, it is very clear, and it is respectfully submitted, that Jerrin has nothing at all to do with applicant's claimed invention. Jerrin is focused on detecting an unauthorized presence and setting an alarm. This is very different than applicant's claimed invention from preventing an intruder who compromises the second network from gaining access to the first network except for the first TCP/IP port. That is, applicant's claimed invention precludes the ability of an intruder to gain access whatsoever, while Jerrin has already given up such a position by recognizing the intruder has already gained unauthorized access and wants to detect such unauthorized access.

The Examiner cites paragraph 102 in Jerrin for the teaching of TCP/IP Port extension using a Gateway methodology, the first TCP/IP port and the second TCP/IP port remain constant and cannot be changed. Referring to paragraph 102 of Jerrin, there is taught flow data collection provides immediate identification of which hosts are acting as a client, a server, and which service that is being utilized. The port profiling engine provides instant notification when hosts in a zone communicate to other zones using an unauthorized service. Zone locking imparts the ability to determine which services they host is authorized to perform when communicating with other zones. Each designated zone has predefined unauthorized zones that are not allowed to attempt to connect to that designated zone as a client. However, particular services can be exempted from the general zone lockout. Consequently, if any unauthorized zone for a particular zone attempt to connect as a client to a server in the particular zone, an alarm will be generated unless the service is excluded from the zone lockout.

It is respectfully submitted that paragraph 102 has nothing at all to do with ports, but instead lockout zones which is very different from applicant's claimed invention.

Furthermore, it is respectfully submitted that zone locking has no basis, let alone explanation as to how it would be applied to the teachings of Richmond. It is respectfully submitted that the Examiner cannot ignore the context in which each of the teachings the Examiner relies upon is found. The controlling of concurrent usage of network resources by multiple users at an entry point to a communication network is very distinct from the use of lockout zones. Accordingly, Richmond and Jerrin should not be able to be combined, and even if they are combined, they fail to meet all the limitations of Claim 15 of applicant.

The Examiner has rejected Claims 8 and 9 as being and patentable over Richmond in view of Jacobson and Jerrim. Applicant respectfully traverses this rejection.

Referring to Jacobson, there is disclosed a network connection blocker, method, and computer readable memory for monitoring connections in a computer network and blocking the unwanted connections. Jacobson teaches a large computer network with subnets that include host computers. The subnets include a protected a subnet that is protected with a network connection blocker and remote subnets that are remotely connected to the protected subnet. The host computers include local host computers that are within the protected subnet and remote host computers that are within the remote subnets. See column 2, line 66 through column 3, line 7.

The protected subnet includes the network connection blocker that is connected to the protected host computers and the local gateway within the subnet by the communication lines of the subnet. The blocker receives all of the packets transmitted between the protected host computers within the protected subnet at all of the packets transmitted between the protected and remote host computers. In doing so, the blocker passively monitors all of the connections between the protected host computers and all of the connections between the protected and remote host computers. And, it actively blocks those of the connections that are not wanted by transmitting packets to the host computers that form the unwanted connections to cause these computers to close the unwanted connections. See column 3, lines 41-55.

As is very clear from the above description, Jacobson teaches that the blocker reviews the packets of all connections that exist between any of the host computers and the protected subnet and the host computers in the remote subnets. There is no teaching or suggestion whatsoever of the architecture of applicant's claimed invention. Specifically, there is no teaching or suggestion of a communication portion connecting the first network and the second network only through the first TCP/IP port and a second TCP/IP port that is constant and cannot be changed and which does not connect the first network and the second network. Instead, Jacobson teaches away from this, by providing unlimited connectivity, with the blocker passively reviewing all the connections.

It is respectfully submitted that Jacobson teaches a totally different approach from policing and protecting a network. Furthermore, to the extent that Jacobson may be applicable, it does not prevent an intruder from accessing any aspect of the protected subnet. Jacobson teaches that after the fact, when the connection already exists, it has to be discovered by the blocker so the blocker can then send out packets to cause a computer to close its unwanted connection. Who knows how much damage could have occurred to the protected subnet in that time. Applicant's claimed invention precludes this from even happening. Thus, it is respectfully submitted that the very teaching that the Examiner relies upon from Jacobson to make it obvious to one skilled in the art to have TCP/IP port extension using Gateway methodology, the first TCP/IP port and the second TCP/IP port remain constant and cannot be changed, prevents an intruder who compromises the second network from gaining access to the first network in order to provide network security by passively monitoring connections between the subnet and the rest of the network and actively blocking those of the connections that are wanted, as the Examiner states on page 5, first full paragraph, teaches away from applicant's claimed invention and does not teach at all with the Examiner purports it to teach.

Accordingly, Claim 15 is patentable over Richmond and Jerrim and Jacobson. Claims 16-22 are dependent to parent Claim 15 and are patentable for the reasons Claim 15 is patentable. Claim 23 is patentable for the reasons Claim 15 is patentable. Claims 24-27 are dependent to Claim 15 and is patentable for the reasons Claim 15 is patentable.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 15-27, now in this application be allowed.

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

9/5/08
Date

Ansel M. Schwartz
Registration No. 30,587

Respectfully submitted,

Ansel M. Schwartz
Reg. No. 30,587
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
Tel.: (412) 621-9222